УДК 518.5

О. В. ТОНІЦА, канд. фіз.-мат. наук, доцент, НТУ «ХПІ»;
І. В. ЄРЕМЕНКО, інженер-програміст ТОВ «Nix Solutions», м. Харків

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СИСТЕМ АНАЛІЗУ БЕЗПЕКИ ТЕХНОЛОГІЧНИХ ОБ'ЄКТІВ

В статті розглядаються конструктивні методи і алгоритми комп'ютерного і математичного моделювання систем аналізу безпеки, які засновані на побудові та аналізі дерева відмов. Запропонований підхід дозволяє виконувати моделювання ризику аварій на основі структурно-логічної схеми виробничого процесу при будь-яких видах завдання ризику збоїв на кожному етапі виробничого процесу.

В статье рассматриваются конструктивные методы и алгоритмы компьютерного и математического моделирования систем анализа безопасности, основанные на построении и анализе дерева отказов. Предложенный подход позволяет выполнять моделирование риска аварий на основе структурно-логической схемы производственного процесса при любых видах задания риска сбоев на каждом этапе производственного процесса.

In the article structural methods and algorithms are examined computer and mathematical designs of the systems of analysis of safety, based on a construction and analysis of tree of refuses. Offered approach allows to execute the design of risk of failures on the basis of structural-logical chart of production process at any types of task of risk of failures on every stage of production process.

Вступ. З огляду на стан сучасної промисловості проведення аналізу небезпеки та оцінки ризику техногенних аварій є пріоритетним напрямком для розвитку усієї галузі. Більшість обладнання та споруд – це спадщина радянських часів, яка вже відробила свій «вік» і знаходиться в аварійному стані. Але разом змінити левову частину виробничої бази навряд є реалістичним та економічно обґрунтованим. Тому процес реорганізації та переоснащення виробництва протікає поступово. Це означає постійний контакт працівників із небезпечними об'єктами та підвищену імовірність виникнення позаштатних ситуацій. До того в Україні розвинуті галузі з підвищеними ризиками: металургійна, коксова, хімічна та інші. Все це спонукає до розроблення систем аналізу безпеки підприємств, які б відповідали сучасним вимогам надійності та продуктивності.

Темпи наукового прогресу дозволяють швидко розвивати методи моделювання та аналізу складних систем, а енергійний розвиток цифрової обчислювальної техніки дозволяє реалізувати ці методи у вигляді автоматизованих систем. У автоматизованих системах управління технологічними процесами і системах протиаварійного автоматичного захисту стало можливим вирішення складних завдань розрахунку, аналізу і прогнозування аварійних ситуацій, моделювання технологічних процесів і отримання багатоваріантних рішень.

Число елементів і параметрів технологічної установки, здатних в тій чи іншій мірі вплинути на виникнення і розвиток аварійної ситуації, залежно від складності процесу може досягати десятків і сотень. У складних системах відмови окремих елементів не завжди приводять до відмови всієї системи, крім того, у складних систем є цілий спектр станів – динамічна рівновага, порушення рівноваги, адаптація до несприятливих ситуацій, небезпечні і критичні ситуації і, нарешті, аварії. У зв'язку з цим аналіз ризику подібних технологічних систем – це достатньо складне завдання, що вимагає знань технології, особливостей елементів системи і взаємозв'язку їх між собою. Розробка, адаптація до умов різних галузей промисловості і подальший розвиток методів кількісної оцінки небезпеки і аналізу поточного ризику при функціонуванні промислових установок і об'єктів – все це входить в обов'язки експерта з аналізу ризику. Зрозуміло, що без ефективних засобів аналізу складних систем навіть кращій спеціаліст не в змозі розв'язати поставлене завдання.

Визначення ризику технологічного процесу належним чином не вирішується і, як правило, підміняється на етапі проектування якісним аналізом надійності системи і можливих наслідків аварій. Тому розробка методів кількісної оцінки небезпеки і аналізу ризику для промислових установок і об'єктів є в даний час актуальною проблемою.

Математична постановка задачі. Задача, що розглядається в статті, формулюється таким чином: є набір зв'язаних об'єктів, які узагальнено представляють крупніший об'єкт (досліджуваний промисловий об'єкт). Ці об'єкти представляються у вигляді дерева, де кожна вершина є подією. Основною характеристикою кожної події є вірогідність відмови (для відомих елементів). Вірогідність може бути у виді константи, задана таблицею або функцією (можливе комбінування). Різні події можуть бути зв'язані операціями кон'юнкції або диз'юнкції. Необхідно програмно знайти «вузькі місця» системи, тобто знайти найбільш вірогідні події (і параметри системи, що приводять до настання цих подій) та програмно побудувати спрощене дерево відмов.

Математична модель і методи розв'язання задачі. У дослідженні безпеки широкого поширення набули діаграми впливи структури, що гілкується, звані «деревом» подій (відмов). Деревом подій називають не орієнтований граф, що не має циклів, є кінцевим і зв'язним. У нім кожна пара вершин має бути зв'язаною (сполученим ланцюгом), проте всі з'єднання не повинні утворювати петель (циклів), тобто містити такі маршрути, вершини яких одночасно є початком одних і кінцем інших ланцюгів [2].

Структура дерева подій зазвичай включає одне, розміщувана зверху небажана подія – подія (аварія, нещасний випадок, катастрофа), яка з'єднується з набором відповідних подій, – передумов (помилок, відмов, несприятливих зовнішніх дій), створюючи певні їх ланцюги або «гілки». «Листям» на гілках дерева подій служать передумови – ініціатори причинних

ланцюгів, що розглядуються як аксіоматичні висхідні події, подальша деталізація яких не доцільна. Як вузли дерева подій можуть використовуватися як окремі події або стани, так і логічні умови їх об'єднання (складання або перемножування).

Побудова дерева відмов. При побудові дерева відмов використовують стандартні символи бульової алгебри та додаткові схеми [1, с. 77]. Виділяють п'ять типів вершин дерева відмов: вершини, що відображують первинні відмови; вершини, що відображують результуючі або вторинні відмови; вершини, що відображують локальні відмови, які не впливають на виникнення інших відмов; вершини, відповідні операції логічного об'єднання випадкових подій (типа «АБО»); вершини, відповідні операції логічного твору випадкових подій (типа «І»).

Побудова дерева відмов передбачає виконання наступних процедур:

- визначення меж системи,
- побудова дерева несправностей,
- якісна оцінка,
- кількісна оцінка.

Основною метою побудови дерева несправностей є символічне представлення умов, що існують в системі, здатних викликати її відмову. Крім того, побудоване дерево дозволяє показати в явному вигляді слабкі місця системи і є наочним засобом уявлення і обґрунтування схвалюваних рішень, а також засобом дослідження компромісних співвідношень або встановлення ступеня відповідності конструкції системи заданим вимогам.

Однією з основних переваг дерев відмов є те, що аналіз обмежується виявленням тільки тих елементів систем і подій, які приводять до відмови або аварії. Щоб визначити вірогідність відмови, необхідно знайти аварійні поєднання, для чого необхідно провести якісний і кількісний аналіз дерева відмов. Структура «дерева відмови» включає одну головну подію (аварію, інцидент), яка з'єднується з набором відповідних нижчестоящих події (помилок, відмов, несприятливих зовнішній дій), створюючи причинні ланцюги.

Аналіз дерева відмов. Аналіз дерева відмов полягає у визначенні умов, мінімально необхідних та достатніх для виникнення головної події [3]. Цей процес полягає у використанні якісної та кількісної оцінки дерева відмов.

Якісний аналіз ґрунтується на використанні так званих мінімальних перетинів дерева невправностей. Перетин визначається як безліч елементарних події, що приводять до небажаного результату. Виявлення мінімальних перетинів потребує великих затрат часу та складний машинний алгоритм [1, с. 89], але значно спрощує дерево відмов для сприйняття людиною. Також потрібно спростити вирази з подіями, що повторюються, використовуючи властивості булевої алгебри, інакше будуть отримані помилкові кількісні оцінки [1, с. 93].

Кількісна оцінка дерева здійснюється за допомогою статичного моделювання або аналітичним методом [1].

Програмна реалізація. Запропонований підхід може бути реалізований як шаблон для моделювання спрощеної системи безпеки будь-яких об'єктів у вигляді динамічного дерева відмов. Це твердження підтверджує реалізоване програмне забезпечення (ПЗ). Програма як вхідні дані приймає безліч усіх первинних подій, які складають повну множину передумов головної події і розбиває цю множину на декілька груп так, щоб всі події в групі могли виконуватися одночасно, не створюючи конфліктів. ПЗ має зв'язати з кожною подією відповідну імовірнісну характеристику, чи то константну, чи імовірнісну залежність; мінімізувати число подій, що повторюються, початкової безлічі подій, оскільки при цьому мінімізується кількість вузлів у дереві відмов які треба обробляти. На виході програма видає імовірнісну оцінку появи головною події, тобто проаналізує всі ланцюги дерева відмов за допомогою інструментів теорії вірогідності. ПЗ було розроблено на платформі .NET на базі операційної системи Windows.

В основі розробки ПЗ лежить математична модель дерева. Дерево − це сукупність елементів, званих вузлами (один з яких визначається як корінь), і стосунків («батьківських»), створюючи ієрархічну структуру вузлів. Вузли можуть бути елементами будь-якого типу. Формально дерево за допомогою рекурсії можна визначити таким чином:

- Один вузол є деревом. Цей же вузол також є коренем цього дерева.
- Нехай N − це вузол, а *T1, T2, ..., Тк* − дерева з корінням *N1, N2, ..., Nk* відповідно. Можна побудувати нове дерево, зробивши N батьком вузлів *N1, N2, ..., Nk*. У цьому дереві N буде коренем, а *T1, T1, ..., Тк* — піддеревами цього кореня. Вузли *N1, N2, ..., Nk* називаються синами вузла N.

Дерево представлене за допомогою масивів. Тобто, якщо T − дерево з вузлами 1, 2 ..., n, то представленням дерева T буде лінійний масив A, де кожен елемент $A[i]$ є покажчиком або курсором на батька вузла і, а корінь дерева T відрізняється від інших вузлів тим, що має нульовий покажчик або покажчик на самого себе як на батька. Дане уявлення використовує властивість дерев, що кожен вузол, відмінний від кореня, має тільки одного батька. Використовуючи це уявлення, батька будь-якого вузла можна знайти за фіксований час. Проходження по будь-якому шляху, тобто перехід по вузлах від батька до батька, можна виконати за час, пропорційний кількості вузлів шляху.

Створення дерева основується на розбитті його на піддерева з не більш ніж двома ієрархічними рівнями. Кожне піддерево оброблюється окремо, починаючи з первинних вузлів, а потім поступово об'єднуються результати, крокуючи до головного вузла (події). Тобто реалізується метод декомпозиції.

Розроблена програма є ефективною, бо її структура є такою, що дії оператора настільки повільні порівняно з виконанням інструкцій програми, що користувач не помічає затримок.

Експериментальні дослідження. Для перевірки розробленої системи розглянемо систему електропостачання (СЕС) кільцевої структури, яка містить 15 елементів: 3 генератори однакової потужності (1, 2, 3); 3 головних розподільних щити ГРЩ (4, 6, 9); 3 перемички (5, 7, 8); 6 вторинних розподільних щитів ВРЩ (10, 11, 12, 13, 14, 15).

Система призначена для забезпечення безперебійного живлення одночасно трьох груп споживачів (П1, П2, П3). Потужності кожного генератора вистачає для забезпечення роботи всіх споживачів. Немає ніяких обмежень по пропускній здатності ні ГРЩ, ні перемичок між ними. Граф-схема системи електропостачання представлена на рис. 1.

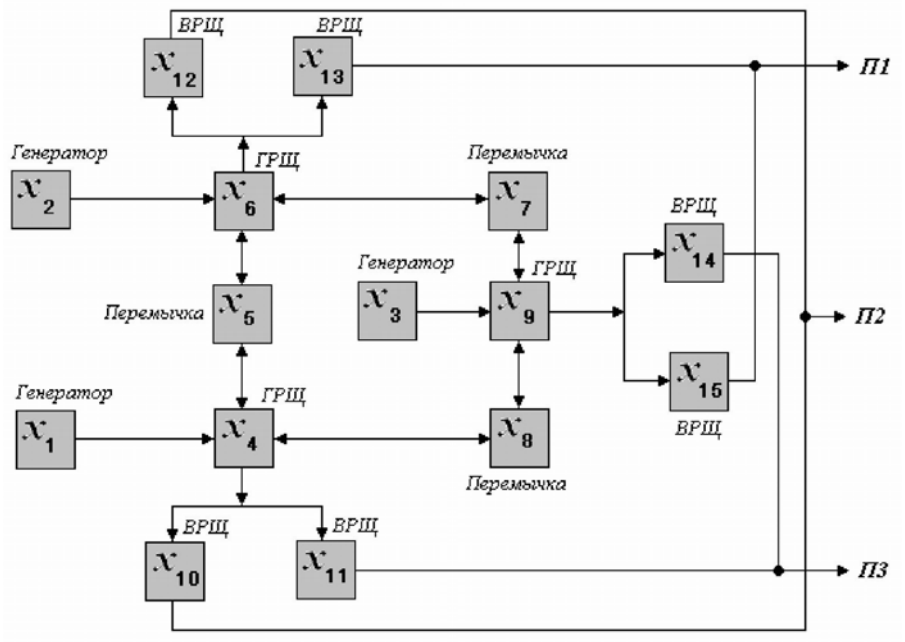

Рис. 1 − Функціональна граф-схема системи електропостачання

Розроблене ПЗ дозволяє моделювати цільову систему за допомогою графічного інтерфейсу. Частина змодельованої системи у вікні розробленої програми показана на рис. 2. Також програма дозволяє побудувати безліч графіків по дослідженню системи, наприклад залежність між вірогідністю справності окремого елемента та всієї системи.

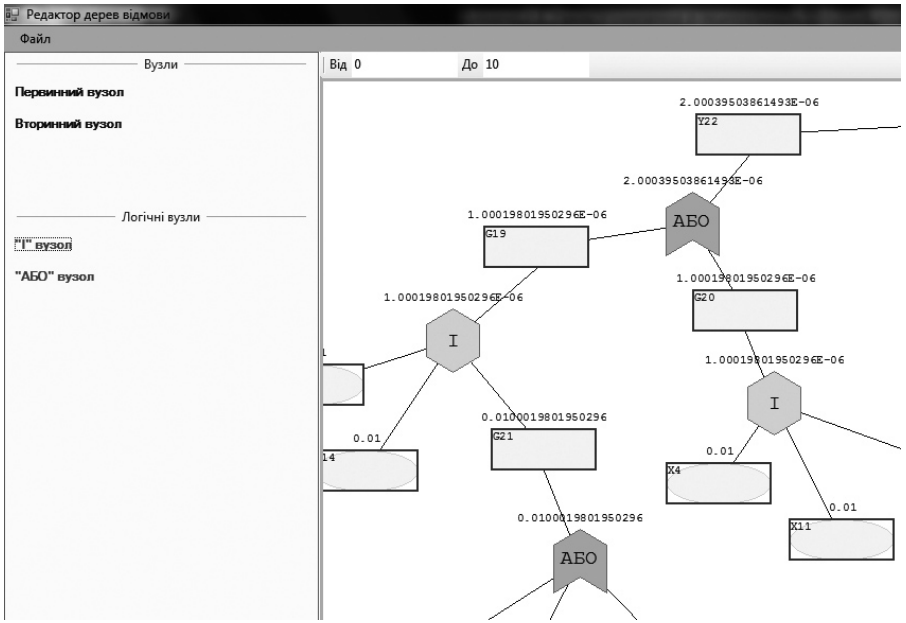

Рис. 2 − Частина дерева відмов для розглянутої системи електропостачання у вікні розробленої програми

Висновки. Запропонований підхід та розроблене ПЗ дозволяє виконувати моделювання ризику аварій на основі структурно-логічної схеми виробничого процесу при будь-яких видах завдання ризику збоїв на кожному етапі виробничого процесу.

Список літератури: 1. *Ветошкин А. Г.* Надёжность технических систем и техногенный риск / *А. Г. Ветошкин.* – Пенза: ПГУАиС, 2003. – С. 74–98. **2.** *Швыряев Ю. В.* Вероятностный анализ безопасности атомных станций. Методика выполнения / *Ю. В. Швыряев.* – М. : ИАЭ им. И. В. Курчатова, 1992. – С. 43–111. **3.** *Белов П. Г.* Теоретические основы системной инженерии безопасности / *П. Г. Белов.* – Киев : КМУГА, 1997. – 426 с.

Надійшла до редколегії 05.11.2010